SI3000 Антифрод

Руководство по установке и настройке

АО «Искра Технологии», май 2024 г. KSS887500-LDR-020

Если используется копия документа, проверьте ее соответствие последней версии документа.

Документ выпущен компанией

АО «Искра Технологии»

ул. Комвузовская, дом 9, строение А,
г. Екатеринбург, РФ 620066

Т: +7 343 210 69 51
Ф: +7 343 341 52 40

info@iskratechno.ru
www.iskratechno.ru

© Искра Технологии, 2024. Все права защищены.

Содержание

1. О документе ... 5
1.1. Назначение ... 5
1.2. Целевая аудитория ... 5
1.3. Структура документа ... 5
1.4. Сопутствующая документация ... 5
1.5. Условные обозначения ... 6
1.5.1. Дополнительная маркировка текста ... 6
1.5.2. Интерфейс командной строки (CLI) ... 6
1.5.3. Графический интерфейс пользователя (GUI) ... 6
1.6. Список сокращений ... 6
2. Общие сведения ... 8
2.1. Компоненты системы ... 8
2.2. Функциональности ... 8
2.3. Варианты конфигурации системы ... 9
2.4. Состав пакета ПО ... 9
2.5. Собственные сервисы ... 10
2.6. Конфигурация установочного скрипта ... 10
3. Инструкции для одиночной конфигурации ... 12
3.1. Предварительные условия для одиночной конфигурации ... 12
3.2. Установка пакета ПО для одиночной конфигурации ... 13
3.3. Лицензирование продукта в одиночной конфигурации ... 13
3.4. Настройка взаимодействия с FMS для одиночной конфигурации ... 14
4. Инструкции для конфигурации высокой доступности ... 16
4.1. Предварительные условия для конфигурации HA ... 16
4.2. Установка ПО на арбитре дублированного узла ... 17
4.3. Проверка работы кластера дублированного узла ... 17
4.4. Лицензирование продукта в конфигурации HA ... 18
4.5. Настройка взаимодействия с FMS для конфигурации HA ... 19
5. Инструкции для конфигурации с георезервированием ... 22
5.1. Предварительные условия для конфигурации GEO ... 22
5.2. Установка ПО на арбитре первой локации ... 23
5.3. Проверка работы кластера первой локации ... 24
5.4. Настройки в веб-интерфейсе первой локации ... 24
5.5. Установка ПО на арбитре второй локации ... 26
5.6. Проверка работы кластера второй локации ... 26
5.7. Проверка статуса второй локации ... 27
5.8. Лицензирование продукта в конфигурации GEO ... 27
5.9. Настройка взаимодействия с FMS для конфигурации GEO ... 27

Список рисунков

Рис. 2.1. Распределение и функции основных компонентов пакета AA6511AX ... 10
Рис. 3.1. Ввод базовых настроек нового одиночного узла ... 14
Рис. 4.1. Базовые настройки дублированного узла в MNS ... 19
Рис. 4.2. Расширенные настройки дублированного узла в MNS ... 20
Рис. 5.1. Назначение идентификационных имен локациям ... 25
Рис. 5.2. Добавление плавающего IP-адреса георезервированного узла ... 25
Рис. 5.3. Выбор состояния для первой локации ... 25
Рис. 5.4. Проверка состояния второй локации ... 27
Рис. 5.5. Базовые настройки дублированного узла первой локации в MNS ... 28

© Искра Технологии, 2024. Все права защищены.

Рис. 5.6. Расширенные настройки дублированного узла первой локации в MNS 29

Список таблиц

Табл. 1.1. Структура документа 5
Табл. 1.2. Сопутствующая документация 5
Табл. 1.3. Условные обозначения для маркировки текста 6
Табл. 1.4. Условные обозначения для описания интерфейса командой строки (CLI) 6
Табл. 1.5. Условные обозначения для описания графического интерфейса пользователя (GUI) 6
Табл. 1.6. Список сокращений на английском языке 6
Табл. 1.7. Список сокращений на русском языке 7
Табл. 2.1. Параметры развертывания в файле node-hosts.yaml 10
Табл. 3.1. Требования к ВМ для продукта «SI3000 Антифрод» в одиночной конфигурации 12
Табл. 4.1. Требования к ВМ для продукта «SI3000 Антифрод» в конфигурации высокой доступности 16
Табл. 5.1. Требования к ВМ для продукта «SI3000 Антифрод» в конфигурации с георезервированием 22

© Искра Технологии, 2024. Все права защищены.

1. О документе

1.1. Назначение

Данный документ содержит инструкции по установке продукта «SI3000 Антифрод» для различных режимов работы системы на виртуальные машины с операционной системой Debian или Astra Linux.

1.2. Целевая аудитория

Документ предназначен для квалифицированных специалистов, ответственных за развёртывание и техобслуживание решений, в состав которых входит продукт «SI3000 Антифрод».

1.3. Структура документа

Табл. 1.1. Структура документа

Глава	Описывает
«Общие сведения»	общее назначение, архитектуру и прочие компоненты решений, в состав которых входит продукт «SI3000 Антифрод».
«Инструкции для одиночной конфигурации»	предварительные условия и поэтапные действия для установки и первичной настройки продукта «SI3000 Антифрод» на машине без резервирования.
«Инструкции для конфигурации высокой доступности»	предварительные условия и поэтапные действия для установки и первичной настройки продукта «SI3000 Антифрод» на дублированном узле.
«Инструкции для конфигурации с георезервированием»	предварительные условия и поэтапные действия для установки и первичной настройки продукта «SI3000 Антифрод» на георезервированном узле.

1.4. Сопутствующая документация

Табл. 1.2. Сопутствующая документация

Код	Название
KSS88750A-LDR	«Руководство администратора (CLI)»
KSS887800-LDR	«Описание системы»
KSS8878L0-LDR	«Инструкции по устранению ошибок»
KSS5420A0-	Пользовательская документация на продукт «SI3000 FMS Система мониторинга неисправностей»
KSS7010A0-	Пользовательская документация на продукт «SI3000 cCS Компактный программный коммутатор»
KSS7110A0-	Пользовательская документация на продукт «SI3000 MNS Система управления и мониторинга»
KSS7970A0-	Пользовательская документация на продукт «SI3000 CS Программный коммутатор»

© Искра Технологии, 2024. Все права защищены.

1.5. Условные обозначения

1.5.1. Дополнительная маркировка текста

Табл. 1.3. Условные обозначения для маркировки текста

Знак	Текст	Описывает
	Предупреждение	Этот знак обозначает текст, который следует прочитать и принять к сведению для недопущения опасных последствий.
	Примечание	Этот знак обозначает дополнительное пояснение.

1.5.2. Интерфейс командной строки (CLI)

Табл. 1.4. Условные обозначения для описания интерфейса командой строки (CLI)

Формат	Описание
Полужирный шрифт	Названия директорий, файлов, параметров.
`Моноширинный шрифт`	Текст командной строки и информация, выводимая на экран.
`Полужирный моноширинный шрифт`	Вводимое значение.

1.5.3. Графический интерфейс пользователя (GUI)

Табл. 1.5. Условные обозначения для описания графического интерфейса пользователя (GUI)

Формат	Описание
Полужирный шрифт	Элементы в окнах приложения: заголовки основных и диалоговых окон, меню, поля данных, кнопки, вкладки...
`Моноширинный шрифт`	Выбираемое или вводимое значение.
>	Угловая скобка указывает на последовательность выбора пунктов меню, функциональных групп и элементов управления, например: **Инвентаризация и топология** > **Узел**.

1.6. Список сокращений

Табл. 1.6. Список сокращений на английском языке

Сокращение	Расшифровка	Описание
cCS	Compact Call Server	Компактный программный коммутатор
COTS	Commercially off-the-shelf	Серийно выпускаемый, свободно доступный на рынке компонент
CS	Call Server	Программный коммутатор
DNS	Domain Name System	Система доменных имен
FMS	Fault Monitoring System	Система мониторинга неисправностей
GEO	Geographically redundant	Географическое резервирование
GUI	Graphical user interface	Графический интерфейс пользователя
HA	High availability	Высокая доступность
HSB	Hot stand-by	Горячее резервирование

© Искра Технологии, 2024. Все права защищены.

Сокращение	Расшифровка	Описание
ID	Identifier, Identification	Идентификатор
IP	Internet protocol	Протокол Интернета
KVM	Kernel-based Virtual Machine	«Виртуальная машина на основе ядра», ПО для виртуализации в среде Linux на платформе x86
LI	Lawful Interception	Средства законного перехвата в телекоммуникационных сетях
MNS	Management Node System	Система управления
NE	Network Element	Сетевой элемент
NEM	Network Element Manager	Менеджер сетевого элемента, приложения для управления конфигурацией CS и т.п
NTP	Network Time Protocol	Протокол сетевого времени
SFTP	SSH File Transfer Protocol	Протокол прикладного уровня передачи файлов, работающий поверх безопасного канала
SSH	Secure Shell	«Защищенная оболочка», протокол для удаленного управления ОС и туннелирования TCP-соединений

Табл. 1.7. Список сокращений на русском языке

Сокращение	Описание
БД	База данных
ВМ	Виртуальная машина
ГБ	Гигабайт
ГРЧЦ	Главный радиочастотный центр
ИС	Информационная система
КВр	Компонент верификации
ОЗУ	Оперативное запоминающее устройство
ОС	Операционная система
ПО	Программное обеспечение
УВз	Узел взаимодействия
УВр	Узел верификации
ФГУП	Федеральное государственное унитарное предприятие
ФЗ	Федеральный закон
ЦП	Центральный процессор
ЦСУ	Центральная система управления
ЦУ	Центральный узел

© Искра Технологии, 2024. Все права защищены.

2. Общие сведения

ИС «Антифрод» – система под централизованным управлением Радиочастотной службы (ФГУП «ГРЧЦ»), предназначенная для противодействия угрозам безопасности, связанным с подменой абонентских номеров (уникальных кодов идентификации) вызывающих абонентов в процессе инициирования и установления соединений в сети связи общего пользования Российской Федерации.

2.1. Компоненты системы

ИС «Антифрод» включает в себя следующие элементы:

- Центральная система управления (ЦСУ) – источник маршрутной, справочной и авторизационной информации. ЦСУ представляет собой Центральный узел (ЦУ) ИС «Антифрод».
- Узлы верификации (УВр) – выполняют верификацию вызовов.
- Узлы взаимодействия (УВз) – обеспечивают связность всех УВр.

Продукт «SI3000 Антифрод» представляет собой реализацию УВр.

Узел верификации, установленный на объекте оператора связи, включает в себя:

- Компонент верификации – ПО, разработанное согласно спецификациям ГРЧЦ, отвечающее за стыковку УВр с ЦСУ. Также он хранит информации о фактах установления соединений в течении 12 месяцев.
- Модуль регистрации и верификации вызовов (сокр. «Модуль верификации») – самостоятельно разработанное ПО, отвечающее за стыковку УВр со станциями оператора связи.
- Веб-интерфейс УВр – графический интерфейс для настройки продукта «SI3000 Антифрод» и выполнения переключения между локациями в случае конфигурации с георезервированием.

В решение, в состав которого входит продукт «SI3000 Антифрод», также входят следующие продукты производства АО «Искра Технологии»:

- SI3000 CS/cCS – программные коммутаторы, т.е. станции SI3000, соединения абонентов которых проходят верификацию.
- SI3000 MNS – Система управления, предназначенная для мониторинга и управления оборудованием, входящим в состав решения.
- SI3000 FMS – Система мониторинга неисправностей, точка сбора данных об аварийных сигналах, обнаруженных на компонентах системы.

2.2. Функциональности

- Регистрация в базе данных статистики исходящих вызовов, верификацию которых может запросить другой УВр.
- Проверка входящих вызовов из других сетей: модуль отправляет запрос в УВР другого оператора связи, которому принадлежит вызывающий абонент и по получении ответа сообщает станции, проключить или разъединить вызов.
- Верификация вызовов: проверка наличия зарегистрированного исходящего вызова от абонента сети своего оператора в ответ на запрос от других УВр.
- Запись статистической информации об обработанных исходящих и входящих вызовах.
- Создание файлов инцидентов, описывающих случаи выявления подмены абонентских номеров.
- Периодическая отправка файлов статистики верификации и отчетов об инцидентах в ЦУ.
- Отправка статистики зарегистрированных вызовов по запросу в ЦУ.
- Обновление справочников нумерации, УВр/УВз и операторов связи согласно полученным от ЦУ данным.

© Искра Технологии, 2024. Все права защищены.

2.3. Варианты конфигурации системы

В зависимости от требований заказчика, заложенных в техническое решение, система может работать в одном из следующих режимов:

- **Одиночная конфигурация (автономная)**: используется только одна машина, т.е. без дублирования. Он отличается минимальными системными требованиями и простотой установки и обслуживания.
- **Конфигурация высокой доступности (HA)**: используется три машины – дублированный узел и узел-арбитр с функциями БД, установщика и репозитория. Такая конфигурация отличается повышенной отказоустойчивостью, но в то же время более сложными процедурами установки и поддержания работоспособности, а также повышенными системными требованиями.
- **Конфигурация с георезервированием (GEO)**: используется шесть машин, так как она представляет собой конфигурацию высокой доступности на двух географически удаленных друг от друга локациях. На каждой локации есть свой арбитр.

Предупреждение! Поскольку ФГУП «ГРЧЦ» не предписывает точных мероприятий по резервированию УВр ИС «Антифрод», в продукте «SI3000 Антифрод» в данный момент не реализована функция синхронизации конфигурационных файлов **/etc/aa6511/config.json** и **/etc/aa6511/vfn_config.json** на машинах дублированной или георезервированной системы. Копирование конфигурационных файлов с активного узла на остальные узлы после внесения в них изменений должно выполняться вручную.

2.4. Состав пакета ПО

В установочном пакете **aa6511ax_top-X.X.X.X.XXX** содержатся следующие программные компоненты:

- AA6511AX – Узел верификации;
- SP6511AX – веб-приложение для управления конфигурацией Узла верификации;
- PostgreSQL (версия 11) – объектно-реляционная система управления базами данных (СУБД);
- Wildfly – сервер приложений;
- Nginx – веб-сервер и почтовый прокси-сервер;
- alarm-tools – набор утилит для выполнения диагностических тестов, сбора и отправки аварийных сигналов;
- etcd – распределенное хранилище типа «ключ-значение» с открытым исходным кодом, которое используется для поддержки работы кластеров;
- Patroni – Python-приложение для создания и функционирования высокодоступных PostgreSQL-кластеров на основе потоковой репликации.
- Пакеты ОС Astra Linux/Debian, которые могут отсутствовать на целевой машине.

© Искра Технологии, 2024. Все права защищены.

Как обозначено в списке, некоторые программные компоненты нужны только в случае дублирования или георезервирования продукта. Например, в конфигурации с георезервированием ПО инсталлируется и используется следующим образом:

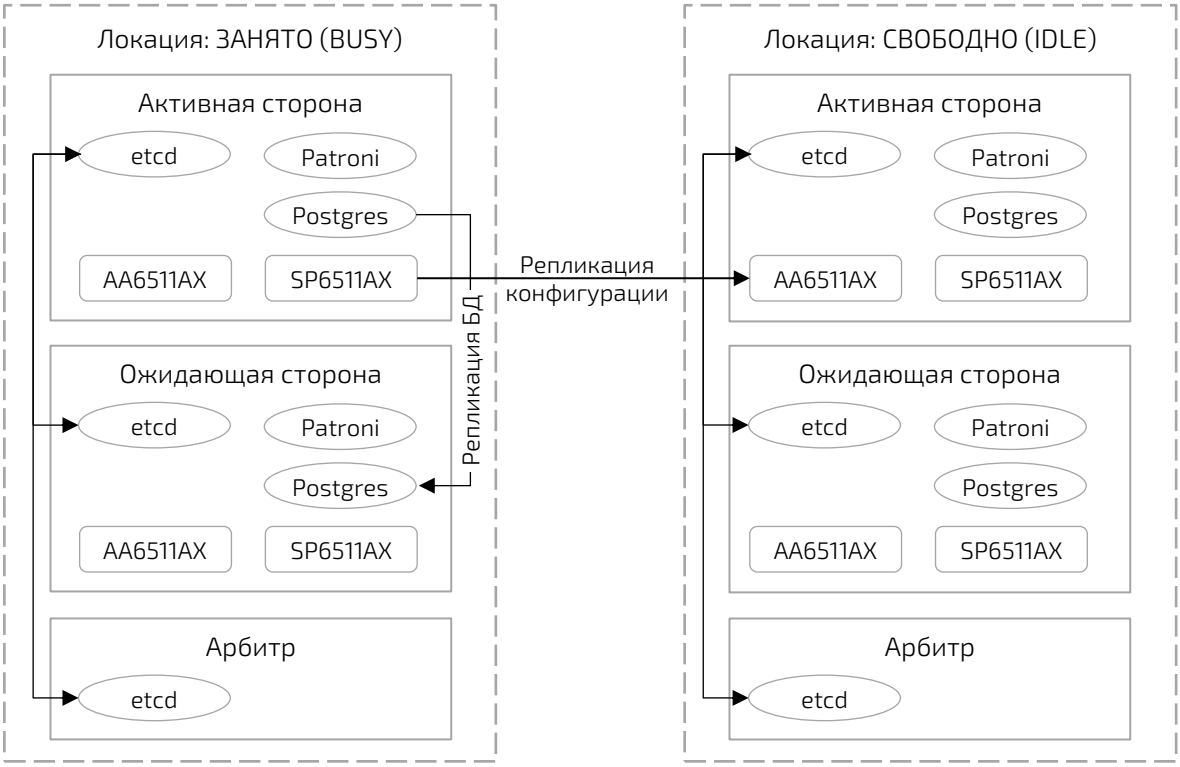

Рис. 2.1. Распределение и функции основных компонентов пакета AA6511AX

2.5. Собственные сервисы

После инсталляции программного пакета на ВМ УВр будут добавлены следующие сервисы, разработанные АО «Искра Технологии»:

- **aa6511.service** – основной сервис Модуля регистрации и верификации вызовов;
- **aa6511-sys-cfg-gen.service** - вспомогательный генератор конфигурации для других сервисов (кроме основного **aa6511.service**);
- **diag-test-runner.service** – сервис для выполнения диагностических тестов;
- **alarm-collector.service** – сервис для сбора аварийных сигналов по результатам диагностических тестов;
- **snmp-cfg-gen.service** – генератор конфигурации для системного сервиса **snmpd.service**, который принимает и обрабатывает запросы от систем мониторинга и других внешних потребителей по протоколу SNMP;
- **fms-snmp-subagent.service** – сервис для отправки аварийных сигналов в SI3000 FMS.

2.6. Конфигурация установочного скрипта

Файл с конфигурацией установочного скрипта находится по пути **install/vars/node-hosts.yaml** в пакете ПО продукта AA6511AX и содержит настройки, представленные в Табл. 2.1:

Табл. 2.1. Параметры развертывания в файле node-hosts.yaml

Раздел/Параметр	Описание
`# all modes settings`	Общие настройки для всех вариантов конфигурации
`ntp_hosts`	Список сетевых имен или IP-адресов серверов синхронизации времени NTP

© Искра Технологии, 2024. Все права защищены.

Раздел/Параметр	Описание
fms_hosts	Список сетевых имен или IP-адресов серверов Системы мониторинга неисправностей FMS.
# HA mode settings	Настройки для конфигурации высокой доступности
node1_mn_ip_addr	IP-адрес интерфейса управления первой стороны дублированного узла
node2_mn_ip_addr	IP-адрес интерфейса управления второй стороны дублированного узла
arbiter_mn_ip_addr	IP-адрес интерфейса управления арбитра текущей локации
ha_mn_float_ip_addr	Плавающий IP-адрес интерфейса управления текущей локации
hsb_enabled	Включение функции горячего резервирования
# single mode settings	Настройки для одиночной конфигурации
single_node_mn_ip_addr	IP-адрес интерфейса управления настраиваемого узла

Пример содержимого YAML-файла:

```
# all modes settings:
ntp_hosts:
  - 192.168.101.69

fms_hosts:
  - 192.168.143.60

# HA mode settings:
node1_mn_ip_addr:  192.168.143.184
node2_mn_ip_addr:  192.168.143.185
arbiter_mn_ip_addr: 192.168.143.186
ha_mn_float_ip_addr: 192.168.143.198

hsb_enabled: true

# single mode settings:
single_node_mn_ip_addr: 1.2.3.4
```

© Искра Технологии, 2024. Все права защищены.

3. Инструкции для одиночной конфигурации

3.1. Предварительные условия для одиночной конфигурации

Сетевое окружение

- В окружении установлены и настроены следующие вспомогательные компоненты производства АО «Искра Технологии»:
  - Система управления SI3000 MNS.
  - Система мониторинга неисправностей SI3000 FMS.
  - Один или несколько сетевых элементов с функциональностью программного коммутатора SI3000 CS/cCS под управлением менеджера NEM.
- IP-адреса и сетевые имена серверов и приложений добавлены на сервер DNS.
- Вам известны все IP-адреса или сетевые имена перечисленных выше, а также сторонних компонентов, которые нужно будет вводить во время процедур инсталляции и первичной настройки решения.

Виртуальная машина

На сервере, предназначенном для продукта «SI3000 Антифрод», создана виртуальная машина со следующими характеристиками:

Табл. 3.1. Требования к ВМ для продукта «SI3000 Антифрод» в одиночной конфигурации

Характеристика	Значение
Аппаратный сервер	COTS, например, HP DL380p Gen9, AMD64
Гипервизор	KVM/VMware/OpenStack
ЦП, ядер	8
ОЗУ, ГБ	32
Место на диске, ГБ	350

Операционная система

На виртуальной машине, предназначенной для продукта, должна быть установлена ОС Astra Linux 1.7.3 (Generic без ядерной защиты) или Debian 10 («Buster»):

- ОС Astra Linux приобретается у официального поставщика.
- Файлы стабильно версии ОС Debian доступна для загрузки на официальном сайте проекта: https://www.debian.org/releases/buster/debian-installer/

Убедитесь, в операционной системе соблюдены следующие требования:

- Добавлена учетная запись с заданным паролем для получения доступа к настройкам и выполнения установочного скрипта, например: пользователь с реквизитами `sysadmin`/`sysadmin`.
- Установлен и настроен пакет **sudo** для получения максимальных прав.
- Верно настроены сетевые параметры:
  - IP – IP-адрес
  - network mask – маска подсети
  - gateway – шлюз
  - hostname – сетевое имя (без доменной части)
  - DNS – данные сервера DNS
  - NTP – данные сервера NTP
  - time zone – часовой пояс

© Искра Технологии, 2024. Все права защищены.

3.2. Установка пакета ПО для одиночной конфигурации

1. Загрузите архивный файл пакета ПО **aa6511ax_top-X.X.X.X.XXX.tar.gz** в определенную директорию на узле верификации.
2. Подключитесь к узлу верификации через клиент SSH с реквизитами, заданными при настройке ОС (например, `sysadmin`/`sysadmin`).
3. Перейдите в директорию с архивным файлом и разархивируйте пакет ПО:
   `tar -xzvf aa6511ax_top-X.X.X.X.XXX.tar.gz`
4. Перейдите в директорию:
   `cd aa6511ax_top-X.X.X.X.XXX/install`
5. Откройте YAML-файл для редактирования:
   `vi vars/node-hosts.yaml`
6. В разделе с общими настройками укажите значения следующих параметров:
   - `ntp_hosts` – IP-адрес или сетевое имя доступного в сети сервера точного времени;
   - `fms_hosts` – IP-адрес или сетевое имя Системы мониторинга неисправностей FMS.
7. В разделе с настройками для одиночной конфигурации укажите:
   - `single_node_mn_ip_addr` – IP-адрес интерфейса управления настраиваемого узла.
8. Запустите развертывание ПО:
   `bash deploy-single.sh`
9. По запросу установочного скрипта введите пароль пользователя ОС:
   ```
   <ssh password> sysadmin
   <BECOME password> sysadmin
   ```
10. После завершения установки удалите временную директорию:
    `sudo rm /tmp/.virtualenvs`
11. Создайте основной файл конфигурации УВр на основе файла-шаблона:
    `sudo cp /etc/aa6511/config.json.example /etc/aa6511/config.json`

Последующая настройка УВр путем редактирования файла конфигурации описана в документе «Руководство администратора» на продукт «SI3000 Антифрод».

3.3. Лицензирование продукта в одиночной конфигурации

1. Подключитесь к узлу верификации через клиент SSH с реквизитами, заданными при настройке ОС (например, `sysadmin`/`sysadmin`).
2. Узнайте уникальный идентификатор ВМ:
   - Откройте файл:
     `cat /var/log/aa6511/AppStat_aa6511_cfc_1.txt`
   - Скопируйте идентификатор, указанный в строке с текстом «This node HWID».
3. Отправьте в компанию-поставщик ПО запрос на лицензию, указав следующие данные:
   - скопированный идентификатор HWID;
   - тип конфигурации;
   - количество подключаемых к УВр станций оператора связи.
4. Проверьте содержимое полученного файла лицензии «license.lic»:
   - `HW Identification 01` – идентификатор HWID;
   - `GEO Anti-fraud Functionality` – отсутствие георезервирования (`false`);
   - `HA Anti-fraud Functionality` – отсутствие дублирования (`false`);
   - `Add Anti-fraud NE` – количество дополнительных станций (т.е. общее количество обслуживаемых станций оператора связи минус 1).
5. Загрузите файл лицензии «license.lic» в директорию **/opt/aa6511/license/** на УВр.

© Искра Технологии, 2024. Все права защищены.

6. Сделайте файл доступным всем пользователям ОС на ВМ УВр:
   `sudo chmod 666 license.lic`

3.4. Настройка взаимодействия с FMS для одиночной конфигурации

1. В веб-браузере откройте страницу входа в веб-приложение MNS по адресу **https://<ip>/mns/**, где **<ip>** — это IP-адрес или сетевое имя Системы управления MNS.
2. Введите **Имя пользователя** и **Пароль** администратора (например, `sysadmin/sysadmin`) и щелкните кнопку **OK**.
3. В области групп и элементов и выберите элемент **Инвентаризация и топология** > **Узел** и щелкните значок **Создать** на панели инструментов.
4. В окне **Узел NE - Создать**:
   - Определите базовые параметры для одиночного узла:
     - **Имя**: имя для обозначения узла в MNS.
     - **Сетевое имя**: сетевое имя или IP-адрес интерфейса управления одиночного узла.
     - **Тип узла**: щелкните значок **Добавить**, выберите значение **AP** из предопределенного списка и щелкните **OK**.
   - Щелкните кнопку **OK**.

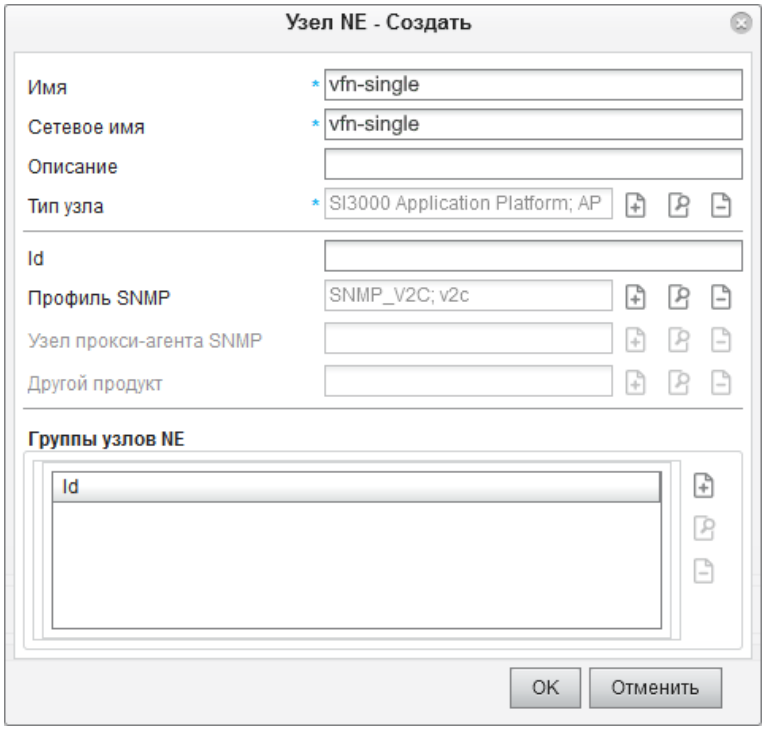

Рис. 3.1. Ввод базовых настроек нового одиночного узла

Если нужно оперативно отслеживать состояние добавленного узла в клиентском приложении SI3000 FMS:

1. В области групп и элементов приложения MNS и выберите элемент **Инвентаризация и топология** > **Дерево версий продукта**.
2. Найдите в древовидной структуре продукт **FMS** > **Fault Monitoring System** и примените к нему команду **Запуск FMS**.
3. Сохраните файл **sso.jnlp** на компьютер и запустите его из браузера или проводника.

© Искра Технологии, 2024. Все права защищены.

Примечание. Если приложение не может запуститься, вручную разрешите сохранение и запуск файла такого типа в браузере, а также добавьте адрес сервера узла MN в список исключений в настройках безопасности **Configure Java**.

Вскоре после запуска Java- приложения откроется главное окно клиента SI3000 FMS.

4. В главном меню выберите **Вид** > **Панель устройств**.
5. В открывшемся окне найдите строку добавленного в MNS узла и перетащите ее на вкладку пользовательского вида в главном окне.

Проверить подключение к FMS можно также на самом сервере FMS с помощью команды вывода списка активных аварийных сигналов:

```
alarmctl show-alarms
```

Пример выдачи:

```
  Code  Description                                              Object Identity  Time
------  -------------------------------------------------------  ---------------  ----------------------
600010  Directory / free space low threshold exceeded            DiagTest/Disk1   2024-03-28 16:53:08.259
600280  Directory / free inodes low threshold exceeded           DiagTest/Disk1   2024-03-28 16:53:08.260
600020  Directory / free space critical threshold exceeded       DiagTest/Disk1   2024-03-28 16:53:08.260
600290  Directory / free inodes critical threshold exceeded      DiagTest/Disk1   2024-03-28 16:53:08.261
```

Примечание. В процессе установки пакета ПО IP-адрес FMS из файла установочного скрипта **node-hosts.yaml** добавляется в файл **/etc/alarm-tools/snmp_config.json**. Поэтому, если этот адрес изменится на другой, нужно заново выполнить инсталляцию пакета или указать новый адрес в JSON-файле, а затем перезапустить сервис **snmp-cfg-gen**.

© Искра Технологии, 2024. Все права защищены.

4. Инструкции для конфигурации высокой доступности

4.1. Предварительные условия для конфигурации HA

Сетевое окружение

- В окружении установлены и настроены следующие вспомогательные компоненты производства АО «Искра Технологии»:
  - Система управления SI3000 MNS.
  - Система мониторинга неисправностей SI3000 FMS.
  - Один или несколько сетевых элементов с функциональностью программного коммутатора SI3000 CS/cCS под управлением менеджера NEM.
- IP-адреса и сетевые имена серверов и приложений добавлены на сервер DNS.
- Вам известны все IP-адреса или сетевые имена перечисленных выше, а также сторонних компонентов, которые нужно будет вводить во время процедур инсталляции и первичной настройки решения.

Виртуальные машины

На серверах, предназначенных для продукта «SI3000 Антифрод», созданы виртуальные машины со следующими характеристиками:

Табл. 4.1. Требования к ВМ для продукта «SI3000 Антифрод» в конфигурации высокой доступности

Имя ВМ	Назначение	ЦП	ОЗУ	Диск
ha_vfn1	Первая сторона дублированного узла	8 ядер	32 ГБ	350 ГБ
ha_vfn2	Вторая сторона дублированного узла	8 ядер	32 ГБ	350 ГБ
ha_vfn0	Арбитр	2 ядра	2 ГБ	60 ГБ
	ИТОГО:	**18 ядер**	**66 ГБ**	**760 ГБ**

Операционная система

На всех виртуальных машинах должна быть установлена ОС Astra Linux 1.7.3 (Generic без ядерной защиты) или Debian 10 («Buster»):

- ОС Astra Linux приобретается у официального поставщика.
- Файлы стабильно версии ОС Debian доступна для загрузки на официальном сайте проекта: https://www.debian.org/releases/buster/debian-installer/

Убедитесь, что в операционной системе соблюдены следующие требования:

- Добавлена одна и та же учетная запись с одинаковым паролем для получения доступа к настройкам и выполнения установочного скрипта, например: пользователь с реквизитами `sysadmin`/`sysadmin`.
- Установлен и настроен пакет **sudo** для получения максимальных прав.
- Запущен сервис **sshd** из установленного пакета **openssh-server**.
- Верно настроены сетевые параметры:
  - IP – IP-адрес
  - network mask – маска подсети
  - gateway – шлюз
  - default route – маршрут по умолчанию 0.0.0.0
  - hostname – сетевое имя (без доменной части), уникальное для каждой ВМ
  - DNS – данные сервера DNS
  - NTP – данные сервера NTP
  - time zone – часовой пояс

© Искра Технологии, 2024. Все права защищены.

4.2. Установка ПО на арбитре дублированного узла

1. Загрузите архивный файл пакета ПО **aa6511ax_top-X.X.X.X.XXX.tar.gz** в определенную директорию на арбитре.
2. Подключитесь к арбитру через клиент SSH с реквизитами, заданными при настройке ОС (например, `sysadmin`/`sysadmin`).
3. Перейдите в директорию с архивным файлом и разархивируйте пакет ПО:
   `tar -xzvf aa6511ax_top-X.X.X.X.XXX.tar.gz`
4. Перейдите в директорию:
   `cd aa6511ax_top-X.X.X.X.XXX/install`
5. Откройте YAML-файл для редактирования:
   `vi vars/node-hosts.yaml`
6. В разделе с общими настройками укажите значения следующих параметров:
   - **`ntp_hosts`** – IP-адрес или сетевое имя доступного в сети сервера точного времени;
   - **`fms_hosts`** – IP-адрес или сетевое имя Системы мониторинга неисправностей FMS.
7. В разделе с настройками для конфигурации высокой доступности укажите значения следующих параметров:
   - **`node1_mn_ip_addr`** – IP-адрес интерфейса управления первой стороны;
   - **`node2_mn_ip_addr`** – IP-адрес интерфейса управления второй стороны;
   - **`arbiter_mn_ip_addr`** – IP-адрес интерфейса управления арбитра;
   - **`ha_mn_float_ip_addr`** – плавающий IP-адрес интерфейса управления дублированного узла;
   - **`hsb_enabled`** – включение функции горячего резервирования (true).
8. Запустите развертывание ПО:
   `bash deploy-ha.sh`

Примечание. Иногда задача по проверке кластера слишком долго не может найти другие узлы и завершается с ошибкой, например:

```
TASK [patroni : Check that the patroni is healthy on the replica server]
    ********************************************************************
    skipping: [192.0.2.25]
    FAILED - RETRYING: Check that the patroni is healthy on the replica server (1200 retries left)
    FAILED - RETRYING: Check that the patroni is healthy on the replica server (1199 retries left)
    ok: [192.0.2.234]
```

В этом случае заново запустите выполнение скрипта, на всякий случай включив функцию расширенного логирования:

`bash -vv deply-ha.sh`

---

9. По запросу установочного скрипта введите пароль пользователя ОС:
   `<BECOME password>` **`sysadmin`**
10. После завершения установки удалите временную директорию инструмента для создания изолированных сред в Python:
    `sudo rm /tmp/.virtualenvs`

4.3. Проверка работы кластера дублированного узла

1. Подключитесь к одной из сторон дублированного узла через клиент SSH с реквизитами, заданными при настройке ОС (например, `sysadmin`/`sysadmin`).
2. Проверьте статус Patroni-кластера командой:
   `sudo patronictl -c /etc/patroni/patroni.yml list`

   Пример выдачи:

```
+---------+-----------------+---------+---------+----+-----------+
| Member  | Host            | Role    | State   | TL | Lag in MB |
```

© Искра Технологии, 2024. Все права защищены.

```
+ Cluster: postgres11-cluster (7284115560707923661)--+-----------+
| ha_vfn1 | 192.168.122.127 | Leader  | running | 34 |           |
| ha_vfn2 | 192.168.122.128 | Replica | running | 34 |         0 |
+---------+-----------------+---------+---------+----+-----------+
```

3. Проверьте функцию переключения активной стороны дублированного узла:
   - Введите команду для принудительного переключения:
     sudo patronictl -c /etc/patroni/patroni.yml switchover
   - Согласитесь с выводимыми данными, нажимая Enter:
     ```
     Master [ha_vfn1]:
     Candidate ['ha_vfn2'] []:
     When should the switchover take place (e.g. 2024-01-17T18:41 )  [now]:
     ```
     Будет показан текущий статус кластера:
     ```
     Current cluster topology
     +---------+-----------------+---------+---------+----+-----------+
     | Member  | Host            | Role    | State   | TL | Lag in MB |
     + Cluster: postgres11-cluster (7284115560707923661)--+-----------+
     | ha_vfn1 | 192.168.122.127 | Leader  | running | 34 |           |
     | ha_vfn2 | 192.168.122.128 | Replica | running | 34 |         0 |
     +---------+-----------------+---------+---------+----+-----------+
     ```
   - Подтвердите запрос на переключения вводом “y” и нажатием Enter:
     ```
     Are you sure you want to switchover cluster postgres11-cluster, demoting
     current master ha_vfn1? [y/N]: y
     ```

   Пример выдачи в случае успешного переключения:
   ```
   2024-01-17 17:41:26.08580 Successfully switched over to "ha_vfn2"
   +---------+-----------------+---------+---------+----+-----------+
   | Member  | Host            | Role    | State   | TL | Lag in MB |
   + Cluster: postgres11-cluster (7284115560707923661)--+-----------+
   | ha_vfn1 | 192.168.122.127 | Replica | stopped |    |   unknown |
   | ha_vfn2 | 192.168.122.128 | Leader  | running | 34 |           |
   +---------+-----------------+---------+---------+----+-----------+
   ```

4.4. Лицензирование продукта в конфигурации HA

1. Подключитесь к одной из сторон дублированного узла через клиент SSH с реквизитами, заданными при настройке ОС (например, **sysadmin**/**sysadmin**).
2. Узнайте аппаратный идентификатор этой стороны:
   - Откройте файл:
     cat /var/log/aa6511/AppStat_aa6511_cfc_*.txt
   - Скопируйте идентификатор, указанный в строке с текстом «This node HWID».
3. Подключитесь к другой стороне дублированного узла через клиент SSH с реквизитами, заданными при настройке ОС.
4. Узнайте аппаратный идентификатор этой стороны:
   - Откройте файл:
     cat /var/log/aa6511/AppStat_aa6511_cfc_*.txt
   - Скопируйте идентификатор, указанный в строке с текстом «This node HWID».
5. Отправьте в компанию-поставщик ПО запрос на лицензию, указав следующие данные:
   - скопированный идентификатор HWID;
   - тип конфигурации;
   - количество подключаемых к УВр станций оператора связи.

© Искра Технологии, 2024. Все права защищены.

6. Проверьте содержимое полученного файла лицензии «license.lic»:
   - `HW Identification 01` – идентификатор HWID;
   - `GEO Anti-fraud Functionality` – отсутствие георезервирования (`false`);
   - `HA Anti-fraud Functionality` – наличие дублирования (`true`);
   - `Add Anti-fraud NE` – количество дополнительных станций (т.е. общее количество обслуживаемых станций оператора связи минус 1).
7. На каждой из сторон дублированного узла:
   - Загрузите файл лицензии «license.lic» в директорию **/opt/aa6511/license/**.
   - Сделайте файл доступным всем пользователям ОС на ВМ УВр:
     `sudo chmod 666 license.lic`

4.5. Настройка взаимодействия с FMS для конфигурации HA

1. В веб-браузере откройте страницу входа в веб-приложение MNS по адресу **https://<ip>/mns/**, где **<ip>** — это IP-адрес или сетевое имя Системы управления MNS.
2. Введите **Имя пользователя** и **Пароль** администратора (например, `sysadmin/sysadmin`) и щелкните кнопку **OK**.
3. В области групп и элементов и выберите элемент **Инвентаризация и топология** > **Узел** и щелкните значок **Создать** на панели инструментов.
4. В окне **Узел NE - Создать**:
   - Определите базовые параметры для дублированного узла:
     - **Имя**: имя для обозначения узла в MNS.
     - **Сетевое имя**: сетевое имя или плавающий IP-адрес интерфейса управления дублированного узла.
     - **Тип узла**: щелкните значок **Добавить**, выберите значение **AP** из предопределенного списка.
   - Щелкните кнопку **OK**.

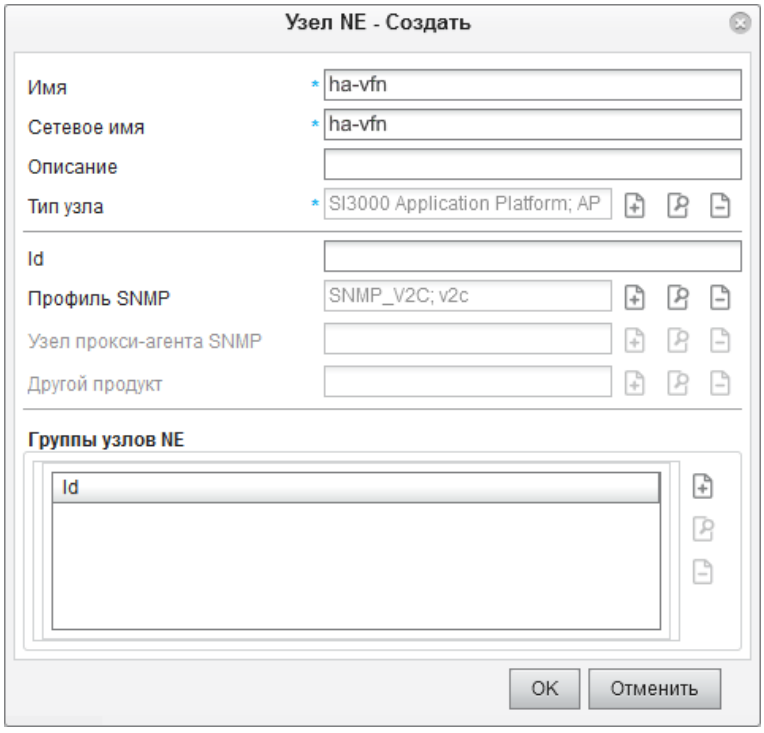

Рис. 4.1. Базовые настройки дублированного узла в MNS

5. В автоматически открывшемся окне **Узел NE - Обновить**:

© Искра Технологии, 2024. Все права защищены.

- В поля **Альтернативное сетевое имя 1** и **Альтернативное сетевое имя 2** введите IP-адреса или сетевые имена интерфейсов управления обеих сторон дублированного узла.
- Щелкните кнопку **OK**.

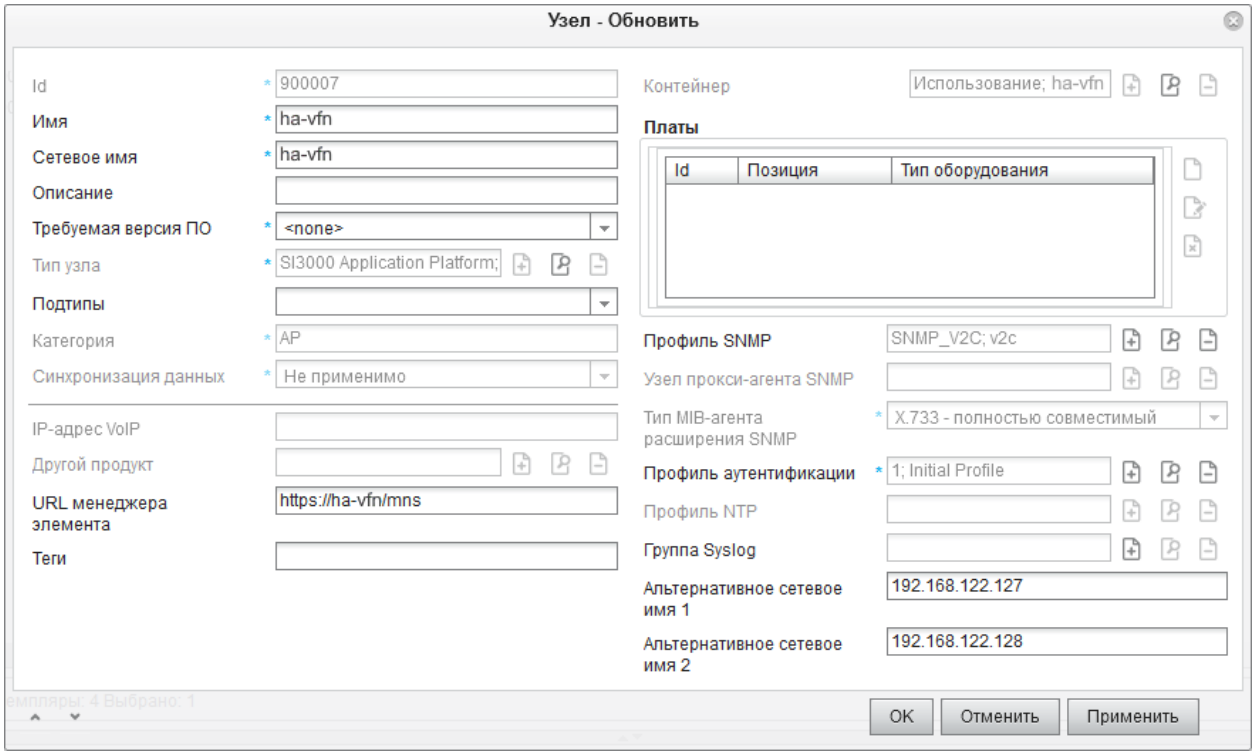

Рис. 4.2. Расширенные настройки дублированного узла в MNS

6. Добавьте узел для узла-арбитра:
   - Щелкните значок **Создать** на панели инструментов.
   - В окне **Узел NE - Создать** определите базовые параметры для узла-арбитра:
     - **Имя**: имя для обозначения узла в MNS.
     - **Сетевое имя**: IP-адрес или сетевое имя узла-арбитра.
     - **Тип узла**: щелкните значок **Добавить**, выберите значение **AP** из предопределенного списка.
   - Щелкните кнопку **OK**.
   - Щелкните **OK** в окне с расширенными настройками узла-арбитра.

Если нужно оперативно отслеживать состояние добавленного узла в клиентском приложении SI3000 FMS:

1. В области групп и элементов приложения MNS и выберите элемент **Инвентаризация и топология** > **Дерево версий продукта**.
2. Найдите в древовидной структуре продукт **FMS** > **Fault Monitoring System** и примените к нему команду **Запуск FMS**.
3. Сохраните файл **sso.jnlp** на компьютер и запустите его из браузера или проводника.

Примечание. Если приложение не может запуститься, вручную разрешите сохранение и запуск файла такого типа в браузере, а также добавьте адрес сервера узла MN в список исключений в настройках безопасности **Configure Java**.

Вскоре после запуска Java- приложения откроется главное окно клиента SI3000 FMS.

4. В главном меню выберите **Вид** > **Панель устройств**.
5. В открывшемся окне найдите строку добавленного в MNS узла и перетащите ее на вкладку пользовательского вида в главном окне.

© Искра Технологии, 2024. Все права защищены.

Проверить подключение к FMS можно также на самом сервере FMS с помощью команды вывода списка активных аварийных сигналов:

```
alarmctl show-alarms
```

Пример выдачи:

```
  Code  Description                                              Object Identity  Time
------  -------------------------------------------------------  ---------------  ----------------------
600010  Directory / free space low threshold exceeded            DiagTest/Disk1   2024-03-28 16:53:08.259
600280  Directory / free inodes low threshold exceeded           DiagTest/Disk1   2024-03-28 16:53:08.260
600020  Directory / free space critical threshold exceeded       DiagTest/Disk1   2024-03-28 16:53:08.260
600010  Directory /boot free space low threshold exceeded        DiagTest/Disk2   2024-03-28 16:53:08.261
600290  Directory / free inodes critical threshold exceeded      DiagTest/Disk1   2024-03-28 16:53:08.261
600290  Directory /boot free inodes critical threshold exceeded  DiagTest/Disk2   2024-03-28 16:53:08.268
600020  Directory /boot free space critical threshold exceeded   DiagTest/Disk2   2024-03-28 16:53:08.269
600280  Directory /boot free inodes low threshold exceeded       DiagTest/Disk2   2024-03-28 16:53:08.273
 50001  Etcd Cluster Degraded                                    DiagTest/etcd    2024-04-12 16:15:09.695
```

Примечание. В процессе установки пакета ПО IP-адрес FMS из файла установочного скрипта **node-hosts.yaml** добавляется в файл **/etc/alarm-tools/snmp_config.json**. Поэтому, если этот адрес изменится на другой, нужно заново выполнить инсталляцию пакета или указать новый адрес в JSON-файле, а затем перезапустить сервис **snmp-cfg-gen**.

© Искра Технологии, 2024. Все права защищены.

5. Инструкции для конфигурации с георезервированием

Инсталляция ПО происходит в два этапа: сначала на первой локации, затем на второй.

5.1. Предварительные условия для конфигурации GEO

Сетевое окружение

- В окружении установлены и настроены следующие вспомогательные компоненты производства АО «Искра Технологии»:
  - Система управления SI3000 MNS.
  - Система мониторинга неисправностей SI3000 FMS.
  - Один или несколько сетевых элементов с функциональностью программного коммутатора SI3000 CS/cCS под управлением менеджера NEM.
- IP-адреса и сетевые имена серверов и приложений добавлены на сервер DNS.
- Вам известны все IP-адреса или сетевые имена перечисленных выше, а также сторонних компонентов, которые нужно будет вводить во время процедур инсталляции и первичной настройки решения.

Виртуальные машины

На серверах, предназначенных для продукта «SI3000 Антифрод», созданы виртуальные машины со следующими характеристиками:

Табл. 5.1. Требования к ВМ для продукта «SI3000 Антифрод» в конфигурации с георезервированием

Имя ВМ	Назначение	ЦП	ОЗУ	Диск
geo_vfn1-1	Первая сторона первой локации	8 ядер	32 ГБ	350 ГБ
geo_vfn1-2	Вторая сторона первой локации	8 ядер	32 ГБ	350 ГБ
geo_vfn1-0	Арбитр первой локации	2 ядра	2 ГБ	60 ГБ
geo_vfn2-1	Первая сторона второй локации	8 ядер	32 ГБ	350 ГБ
geo_vfn2-2	Вторая сторона второй локации	8 ядер	32 ГБ	350 ГБ
geo_vfn2-0	Арбитр второй локации	2 ядра	2 ГБ	60 ГБ
	ИТОГО:	**36 ядер**	**132 ГБ**	**1520 ГБ**

Операционная система

На всех виртуальных машинах должна быть установлена ОС Astra Linux 1.7.3 (Generic без ядерной защиты) или Debian 10 («Buster»):

- ОС Astra Linux приобретается у официального поставщика.
- Файлы стабильно версии ОС Debian доступна для загрузки на официальном сайте проекта: https://www.debian.org/releases/buster/debian-installer/

Убедитесь, что в операционной системе соблюдены следующие требования:

- Добавлена одна и та же учетная запись с одинаковым паролем для получения доступа к настройкам и выполнения установочного скрипта, например: пользователь с реквизитами `sysadmin`/`sysadmin`.
- Установлен и настроен пакет **sudo** для получения максимальных прав.
- Запущен сервис **sshd** из установленного пакета **openssh-server**.
- Верно настроены сетевые параметры:
  - IP – IP-адрес
  - network mask – маска подсети
  - gateway – шлюз

© Искра Технологии, 2024. Все права защищены.

- default route – маршрут по умолчанию 0.0.0.0
- hostname – сетевое имя (без доменной части), уникальное для каждой ВМ
- DNS – данные сервера DNS
- NTP – данные сервера NTP
- time zone – часовой пояс

5.2. Установка ПО на арбитре первой локации

1. Загрузите архивный файл пакета ПО **aa6511ax_top-X.X.X.X.XXX.tar.gz** в определенную директорию на арбитре первой локации.
2. Подключитесь к арбитру через клиент SSH с реквизитами, заданными при настройке ОС (например, `sysadmin`/`sysadmin`).
3. Перейдите в директорию с архивным файлом и разархивируйте пакет ПО:
   `tar -xzvf aa6511ax_top-X.X.X.X.XXX.tar.gz`
4. Перейдите в директорию:
   `cd aa6511ax_top-X.X.X.X.XXX/install`
5. Откройте YAML-файл для редактирования:
   `vi vars/node-hosts.yaml`
6. В разделе с общими настройками укажите значения следующих параметров:
   - **ntp_hosts** – IP-адрес или сетевое имя доступного в сети сервера точного времени;
   - **fms_hosts** – IP-адрес или сетевое имя Системы мониторинга неисправностей FMS.
7. В разделе с настройками для конфигурации высокой доступности укажите значения следующих параметров:
   - **node1_mn_ip_addr** – IP-адрес интерфейса управления первой стороны первой локации;
   - **node2_mn_ip_addr** – IP-адрес интерфейса управления второй стороны первой локации;
   - **arbiter_mn_ip_addr** – IP-адрес интерфейса управления арбитра первой локации;
   - **ha_mn_float_ip_addr** – плавающий IP-адрес интерфейса управления дублированного узла первой локации;
   - **hsb_enabled** – включение функции горячего резервирования (`true`).
8. Запустите развертывание ПО:
   `bash deploy-ha.sh`

Примечание. Иногда задача по проверке кластера слишком долго не может найти другие узлы и завершается с ошибкой, например:

```
TASK [patroni : Check that the patroni is healthy on the replica server]
    ********************************************************************
    skipping: [192.0.2.25]
    FAILED - RETRYING: Check that the patroni is healthy on the replica server (1200 retries left)
    FAILED - RETRYING: Check that the patroni is healthy on the replica server (1199 retries left)
    ok: [192.0.2.234]
```

В этом случае заново запустите выполнение скрипта, на всякий случай включив функцию расширенного логирования:

`bash -vv deply-ha.sh`

9. По запросу установочного скрипта введите пароль пользователя ОС:
   `<BECOME password>` **`sysadmin`**
10. После завершения установки удалите временную директорию инструмента для создания изолированных сред в Python:
    `sudo rm /tmp/.virtualenvs`

© Искра Технологии, 2024. Все права защищены.

5.3. Проверка работы кластера первой локации

1. Подключитесь к одной из сторон дублированного узла через клиент SSH с реквизитами, заданными при настройке ОС (например, **sysadmin**/**sysadmin**).
2. Проверьте статус Patroni-кластера командой:
   sudo patronictl -c /etc/patroni/patroni.yml list

   Пример выдачи:
   ```
   +-------------+-----------------+---------+---------+----+-----------+
   | Member      | Host            | Role    | State   | TL | Lag in MB |
   + Cluster: postgres11-cluster (7284115560707923661) +----+-----------+
   | geo_vfn1-1  | 192.168.122.127 | Leader  | running | 34 |           |
   | geo_vfn1-2  | 192.168.122.128 | Replica | running | 34 |         0 |
   +-------------+-----------------+---------+---------+----+-----------+
   ```
3. Проверьте функцию переключения активной стороны дублированного узла:
   - Введите команду для принудительного переключения:
     sudo patronictl -c /etc/patroni/patroni.yml switchover
   - Согласитесь с выводимыми данными, нажимая Enter:
     ```
     Master [geo_vfn1-1]:
     Candidate ['geo_vfn1-2'] []:
     When should the switchover take place (e.g. 2024-01-17T18:41 )  [now]:
     ```
     Будет показан текущий статус кластера:
     ```
     Current cluster topology
     +-------------+-----------------+---------+---------+----+-----------+
     | Member      | Host            | Role    | State   | TL | Lag in MB |
     + Cluster: postgres11-cluster (7284115560707923661) +----+-----------+
     | geo_vfn1-1  | 192.168.122.127 | Leader  | running | 34 |           |
     | geo_vfn1-2  | 192.168.122.128 | Replica | running | 34 |         0 |
     +-------------+-----------------+---------+---------+----+-----------+
     ```
   - Подтвердите запрос на переключения вводом “y” и нажатием Enter:
     ```
     Are you sure you want to switchover cluster postgres11-cluster, demoting
     current master geo_vfn1-1? [y/N]: y
     ```

   Пример выдачи в случае успешного переключения:
   ```
   2024-01-17 17:41:26.08580 Successfully switched over to "geo_vfn1-2"
   +-------------+-----------------+---------+---------+----+-----------+
   | Member      | Host            | Role    | State   | TL | Lag in MB |
   + Cluster: postgres11-cluster (7284115560707923661) +----+-----------+
   | geo_vfn1-1  | 192.168.122.127 | Replica | stopped |    |   unknown |
   | geo_vfn1-2  | 192.168.122.128 | Leader  | running | 34 |           |
   +-------------+-----------------+---------+---------+----+-----------+
   ```

5.4. Настройки в веб-интерфейсе первой локации

1. Подключитесь к одной из сторон дублированного узла первой локации через клиент SSH с реквизитами, заданными при настройке ОС (например, **sysadmin**/**sysadmin**).
2. Узнайте имя сетевого интерфейса с помощью команды (как правило, это единственный интерфейс, отличный от локального виртуального интерфейса «lo»):
   ip -br addr

© Искра Технологии, 2024. Все права защищены.

Пример выдачи:

```
lo               UNKNOWN        127.0.0.1/8 ::1/128
ens3             UP             192.168.143.181/24 fe80::5054:ff:fef4:4bb5/64
```

3. В веб-браузере откройте страницу входа в веб-приложение «SI3000 Антифрод» по адресу **http://<ip>/gui/**, где **<ip>** — это плавающий IP-адрес первой локации.
4. Введите **Имя пользователя** и **Пароль** первичного администратора (по умолчанию `mnadmin/mnadmin`) и щелкните кнопку **Войти**.
5. В меню навигации выберите пункт **Конфигурация резервирования** и задайте идентификационные имена для обеих локаций:

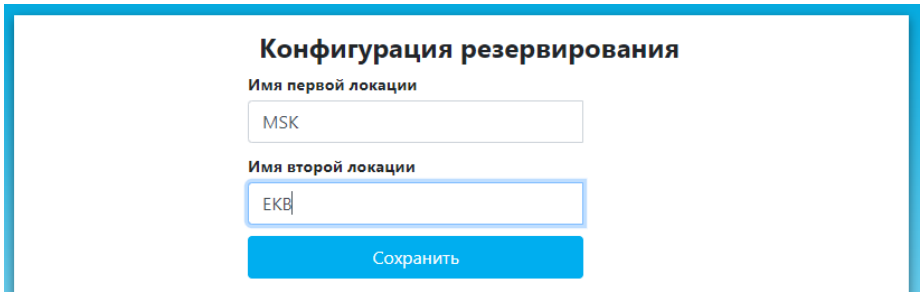

Рис. 5.1. Назначение идентификационных имен локациям

6. В меню навигации выберите пункт **IP-адреса** и добавьте в список плавающий IP-адрес интерфейса управления для георезервированного узла:
   - Щелкните кнопку **Добавить IP-адрес**.
   - В появившемся окне введите значения следующих параметров:
     - **IP-адрес**: плавающий адрес георезервированного узла.
     - **Маска подсети**: маска подсети для указанного IP-адреса.
     - **Имя интерфейса**: имя сетевого интерфейса на четырех сторонах георезервированного узла.
     - **Тип адреса**: `GEO-float`
   - Щелкните кнопку **Сохранить**.

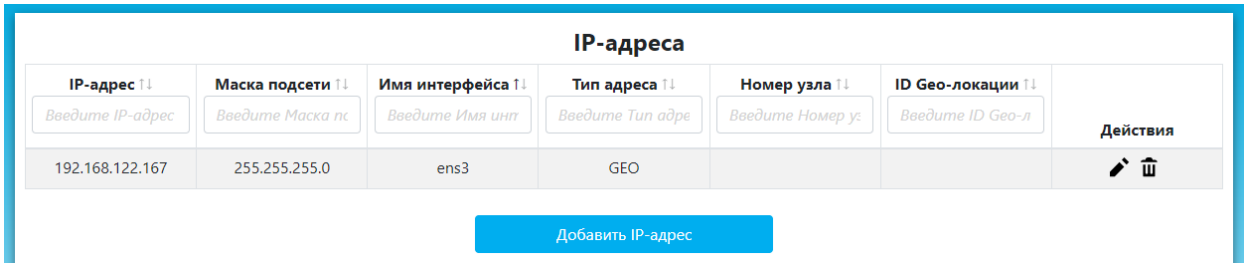

Рис. 5.2. Добавление плавающего IP-адреса георезервированного узла

7. В меню навигации выберите пункт **Геопереключение** и переведите локацию в занятое состояние:
   - В списке **Статус текущей локации** выберите значение **Busy**.
   - Щелкните кнопку **Сохранить**.

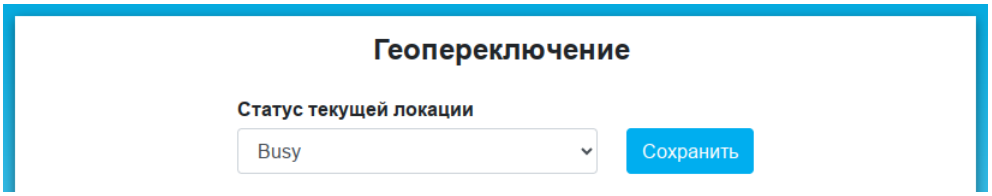

Рис. 5.3. Выбор состояния для первой локации

© Искра Технологии, 2024. Все права защищены.

Первая локация готова к работе. Система уже работает в режиме высокой доступности.

5.5. Установка ПО на арбитре второй локации

1. Загрузите архивный файл пакета ПО **aa6511ax_top-X.X.X.X.XXX.tar.gz** в определенную директорию на арбитре второй локации.
2. Подключитесь к арбитру через клиент SSH с реквизитами, заданными при настройке ОС (например, `sysadmin`/`sysadmin`).
3. Перейдите в директорию с архивным файлом и разархивируйте пакет ПО:
   `tar -xzvf aa6511ax_top-X.X.X.X.XXX.tar.gz`
4. Перейдите в директорию:
   `cd aa6511ax_top-X.X.X.X.XXX/install`
5. Откройте YAML-файл для редактирования:
   `vi vars/node-hosts.yaml`
6. В разделе с общими настройками укажите значения следующих параметров:
   - **`ntp_hosts`** – IP-адрес или сетевое имя доступного в сети сервера точного времени;
   - **`fms_hosts`** – IP-адрес или сетевое имя Системы мониторинга неисправностей FMS.
7. В разделе с настройками для конфигурации высокой доступности укажите значения следующих параметров:
   - **`node1_mn_ip_addr`** – IP-адрес интерфейса управления первой стороны второй локации;
   - **`node2_mn_ip_addr`** – IP-адрес интерфейса управления второй стороны второй локации;
   - **`arbiter_mn_ip_addr`** – IP-адрес интерфейса управления арбитра второй локации;
   - **`ha_mn_float_ip_addr`** – плавающий IP-адрес интерфейса управления дублированного узла второй локации;
   - **`hsb_enabled`** – включение функции горячего резервирования (true).
8. Запустите развертывание ПО:
   `bash deploy-ha.sh`

Примечание. Иногда задача по проверке кластера слишком долго не может найти другие узлы и завершается с ошибкой, например:

```
TASK [patroni : Check that the patroni is healthy on the replica server]
    ********************************************************************
    skipping: [192.0.2.25]
    FAILED - RETRYING: Check that the patroni is healthy on the replica server (1200 retries left)
    FAILED - RETRYING: Check that the patroni is healthy on the replica server (1199 retries left)
    ok: [192.0.2.234]
```

В этом случае заново запустите выполнение скрипта, на всякий случай включив функцию расширенного логирования:

`bash -vv deply-ha.sh`

9. По запросу установочного скрипта введите пароль пользователя ОС:
   `<BECOME password>` **`sysadmin`**
10. После завершения установки удалите временную директорию инструмента для создания изолированных сред в Python:
    `sudo rm /tmp/.virtualenvs`

5.6. Проверка работы кластера второй локации

Проверка выполняется аналогичным образом, что и для первой локации.

© Искра Технологии, 2024. Все права защищены.

5.7. Проверка статуса второй локации

1. В веб-браузере откройте страницу входа в веб-приложение «SI3000 Антифрод» по адресу **http://<ip>/gui/**, где **<ip>** — это плавающий IP-адрес второй локации.
2. Введите **Имя пользователя** и **Пароль** первичного администратора (по умолчанию mnadmin/mnadmin) и щелкните кнопку **Войти**.
3. В меню навигации выберите пункт **Геопереключение** и проверьте, что вторая локация в состоянии Idle («свободно»):

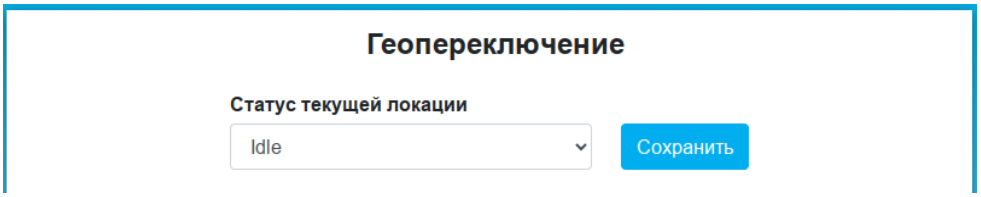

Рис. 5.4. Проверка состояния второй локации

5.8. Лицензирование продукта в конфигурации GEO

1. Узнайте аппаратный идентификатор каждой из четырех сторон георезрвированного узла:
   - Подключитесь к узлу через клиент SSH с реквизитами, заданными при настройке ОС (например, `sysadmin`/`sysadmin`).
   - Откройте файл:
     `cat /var/log/aa6511/AppStat_aa6511_cfc_*.txt`
   - Скопируйте идентификатор, указанный в строке с текстом «This node HWID».
2. Отправьте в компанию-поставщик ПО запрос на лицензию, указав следующие данные:
   - скопированный идентификатор HWID;
   - тип конфигурации;
   - количество подключаемых к УВр станций оператора связи.
3. Проверьте содержимое полученного файла лицензии «license.lic»:
   - `HW Identification 01` – идентификатор HWID;
   - `GEO Anti-fraud Functionality` – наличие георезервирования (`true`);
   - `HA Anti-fraud Functionality` – наличие дублирования (`true`);
   - `Add Anti-fraud NE` – количество дополнительных станций (т.е. общее количество обслуживаемых станций оператора связи минус 1).
4. На каждой из сторон георезервированного узла:
   - Загрузите файл лицензии «license.lic» в директорию **/opt/aa6511/license/**.
   - Сделайте файл доступным всем пользователям ОС на ВМ УВр:
     `sudo chmod 666 license.lic`

5.9. Настройка взаимодействия с FMS для конфигурации GEO

1. В веб-браузере откройте страницу входа в веб-приложение MNS по адресу **https://<ip>/mns/**, где **<ip>** — это IP-адрес или сетевое имя Системы управления MNS.
2. Введите **Имя пользователя** и **Пароль** администратора (например, `sysadmin/sysadmin`) и щелкните кнопку **OK**.
3. В области групп и элементов и выберите элемент **Инвентаризация и топология** > **Узел** и щелкните значок **Создать** на панели инструментов.
4. В окне **Узел NE - Создать**:
   - Определите базовые параметры для дублированного узла первой локации:
     - **Имя**: имя для обозначения узла в MNS.

© Искра Технологии, 2024. Все права защищены.

- **Сетевое имя**: сетевое имя или плавающий IP-адрес интерфейса управления дублированного узла первой локации.
- **Тип узла**: щелкните значок **Добавить** , выберите значение **AP** из предопределенного списка.

- Щелкните кнопку **OK**.

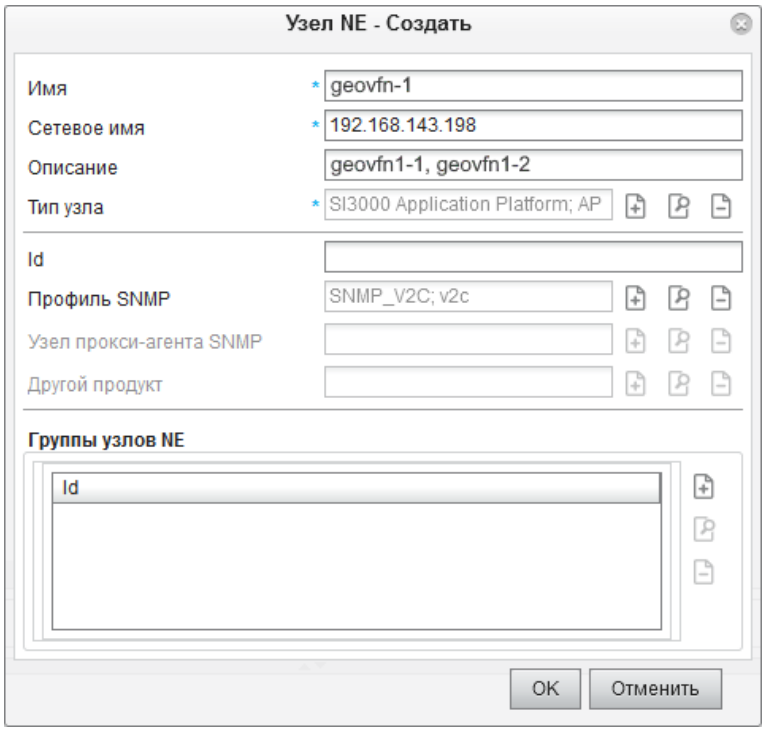

Рис. 5.5. Базовые настройки дублированного узла первой локации в MNS

5. В автоматически открывшемся окне **Узел NE - Обновить**:
   - В поля **Альтернативное сетевое имя 1** и **Альтернативное сетевое имя 2** введите IP-адреса или сетевые имена интерфейсов управления обеих сторон дублированного узла первой локации.
   - Щелкните кнопку **OK**.

© Искра Технологии, 2024. Все права защищены.

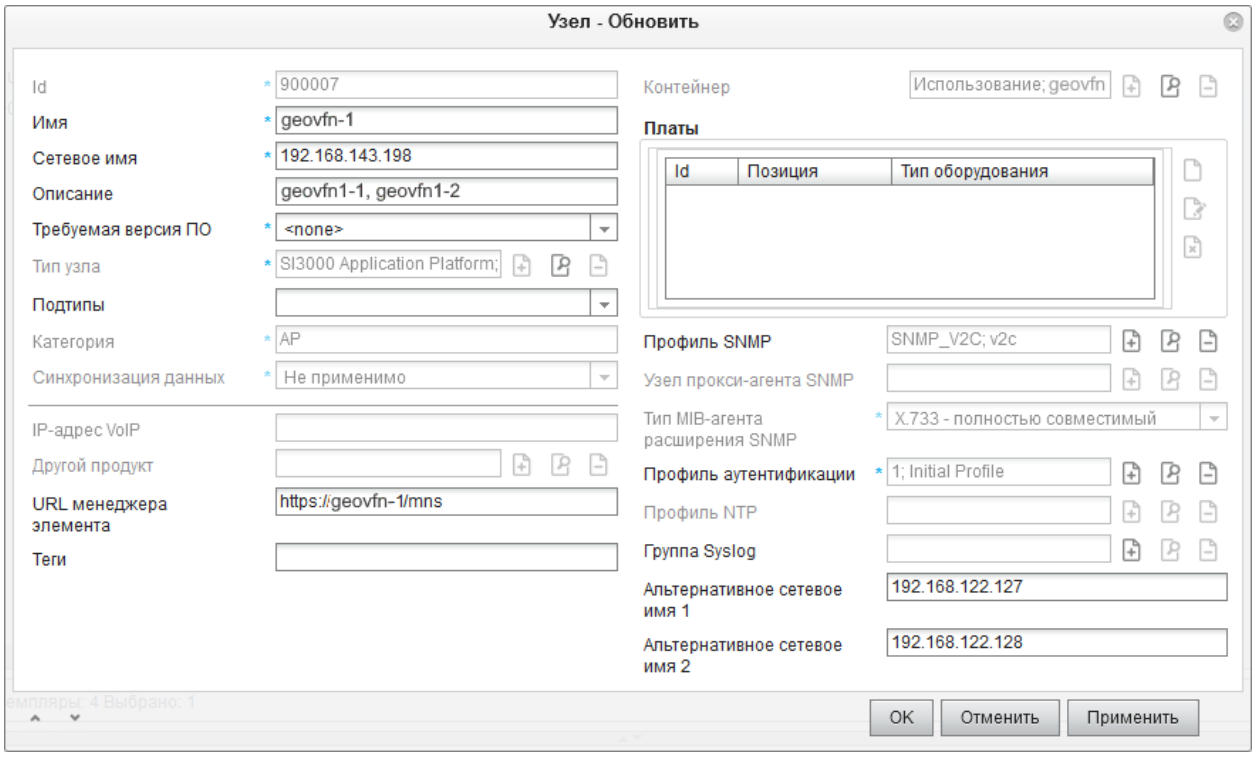

Рис. 5.6. Расширенные настройки дублированного узла первой локации в MNS

6. Добавьте узел для узла-арбитра первой локации:
   - Щелкните значок **Создать** на панели инструментов.
   - В окне **Узел NE - Создать** введите базовые параметры узла-арбитра:
     - **Имя**: имя для обозначения узла в MNS.
     - **Сетевое имя**: IP-адрес или сетевое имя узла-арбитра первой локации.
     - **Тип узла**: щелкните значок **Добавить**, выберите значение **AP** из предопределенного списка.
   - Щелкните кнопку **OK**.
   - Щелкните **OK** в окне с расширенными настройками узла-арбитра.
7. Аналогичным образом добавьте в MNS данные дублированного узел и узла-арбитра второй локации.

Если нужно оперативно отслеживать состояние добавленного узла в клиентском приложении SI3000 FMS:

1. В области групп и элементов приложения MNS и выберите элемент **Инвентаризация и топология** > **Дерево версий продукта**.
2. Найдите в древовидной структуре продукт **FMS** > **Fault Monitoring System** и примените к нему команду **Запуск FMS**.
3. Сохраните файл **sso.jnlp** на компьютер и запустите его из браузера или проводника.

Примечание. Если приложение не может запуститься, вручную разрешите сохранение и запуск файла такого типа в браузере, а также добавьте адрес сервера узла MN в список исключений в настройках безопасности **Configure Java**.

Вскоре после запуска Java- приложения откроется главное окно клиента SI3000 FMS.

4. В главном меню выберите **Вид** > **Панель устройств**.
5. В открывшемся окне найдите строку добавленного в MNS узла и перетащите ее на вкладку пользовательского вида в главном окне.

© Искра Технологии, 2024. Все права защищены.

Проверить подключение к FMS можно также на самом сервере FMS с помощью команды вывода списка активных аварийных сигналов:

```
alarmctl show-alarms
```

Пример выдачи:

```
  Code  Description                                              Object Identity  Time
------  -------------------------------------------------------  ---------------  ----------------------
600010  Directory / free space low threshold exceeded            DiagTest/Disk1   2024-03-28 16:53:08.259
600280  Directory / free inodes low threshold exceeded           DiagTest/Disk1   2024-03-28 16:53:08.260
600020  Directory / free space critical threshold exceeded       DiagTest/Disk1   2024-03-28 16:53:08.260
600010  Directory /boot free space low threshold exceeded        DiagTest/Disk2   2024-03-28 16:53:08.261
600290  Directory / free inodes critical threshold exceeded      DiagTest/Disk1   2024-03-28 16:53:08.261
600290  Directory /boot free inodes critical threshold exceeded  DiagTest/Disk2   2024-03-28 16:53:08.268
600020  Directory /boot free space critical threshold exceeded   DiagTest/Disk2   2024-03-28 16:53:08.269
600280  Directory /boot free inodes low threshold exceeded       DiagTest/Disk2   2024-03-28 16:53:08.273
 50001  Etcd Cluster Degraded                                    DiagTest/etcd    2024-04-12 16:15:09.695
```

Примечание. В процессе установки пакета ПО IP-адрес FMS из файла установочного скрипта **node-hosts.yaml** добавляется в файл **/etc/alarm-tools/snmp_config.json**. Поэтому, если этот адрес изменится на другой, нужно заново выполнить инсталляцию пакета или указать новый адрес в JSON-файле, а затем перезапустить сервис **snmp-cfg-gen**.

© Искра Технологии, 2024. Все права защищены.